UTM機能概要

SRX UTM

アンチウィルス – カスペルスキー

- Express AV – パケットベース, ハイスピードAVソリューション
- Full AV – HTTP, FTP, SMTP, POP, IMAPのファイルに添付されているウィルスをスキャンするためのファイルベースのAV (ScreenOSと同様)

ウェブ フィルタリング – サーフコントロール/ウェブセンス

- 統合型WF - 40種類のカテゴリーからURLアクセスをコントロール
- リダイレクト型WF - ローカルにウェブセンスのサーバを構築し、リダイレクトさせることにより、URLアクセスをコントロール

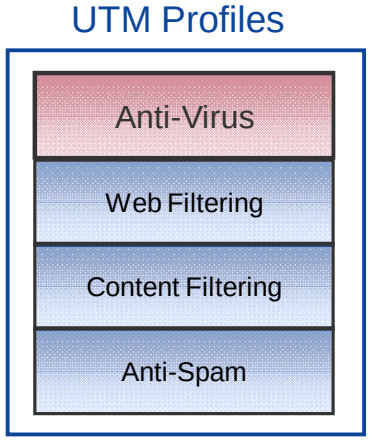
アンチスパム – シマンテック

- IPベースのサービス
- メールアドレスまたは、ドメイン名でのブラックリスト/ホワイトリスト

コンテンツ フィルタリング

- プロトコルコマンド、ファイルの拡張子、MIMEタイプによりトラフィックをコントロール
- DLP (Data Loss Prevention) 技術
- キーワードマッチング (注:ロードマップ)

アンチウィルス



2つのAVエンジンを用意

- Full AV– ファイルベース
- Express AV – パケット(RegEX)ベース
- Full AVとExpress AVは同時利用不可。(切り替えには要リブート)
- 一つのライセンスで、2つのエンジンの切り替えができます。

2つのエンジンの使い分け

- AVは、CPUプロセスに大きなインパクトがあります。
- ハイメモリー版SRXには、プロセスをオフロードできるRegEXハードウェアアクセラレーターを搭載しています。
- ストリングベースのエンジンを採用しているExpress AVは、パフォーマンスの向上に、重きを置いています。
- Express AVでは、多種多様なウィルスを検知できない場合があります。その際には、Full AVを必要とするケースも存在します。

FULL AV VS. EXPRESS AV <1>

パフォーマンス

- Express AVは、ウィルス処理をハードウェアチップにオフロードしているため、Full AVよりも高いパフォーマンスを発揮できます。

シグネチャー数

- Express AVの1万シグネチャーに対し、Full AVは45万シグネチャーを保持しています。

メモリ使用率

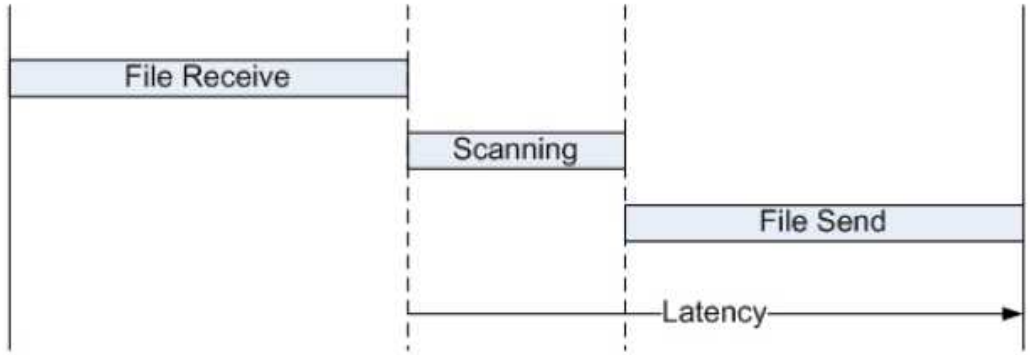
- Express AVは、80MB RAM以下、FLASHを10MB使用します。

Full AV と Express AVの使い分け

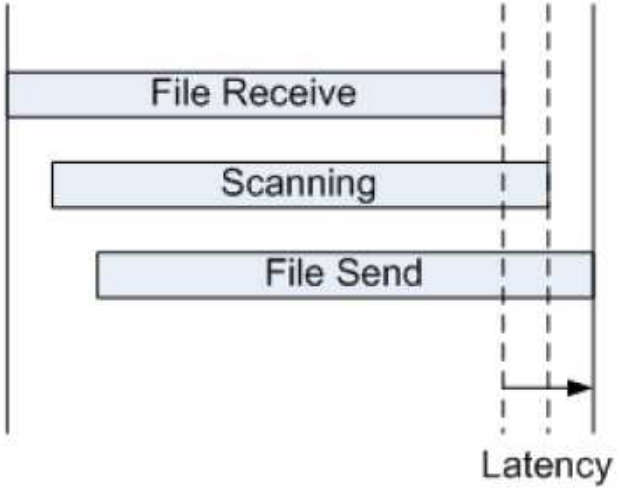
- パフォーマンスを求めるのであれば、Express AVをお勧めします。
- 厳格に、ウィスルを対処したい場合には、Full AVをお勧めします。

FULL AV VS. EXPRESS AV <2>

Full AV



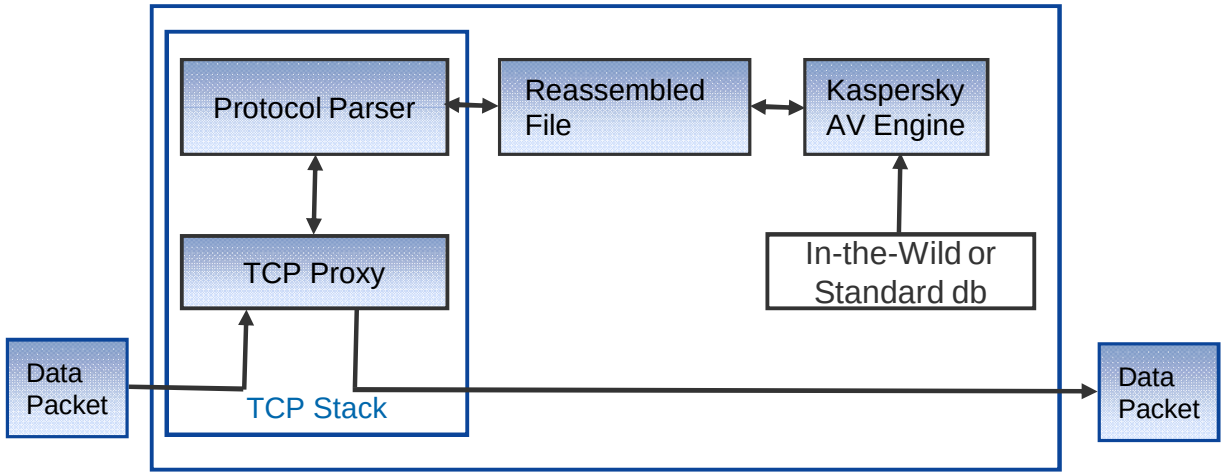
Express AV



FULL AV & EXPRESS AV ソリューション

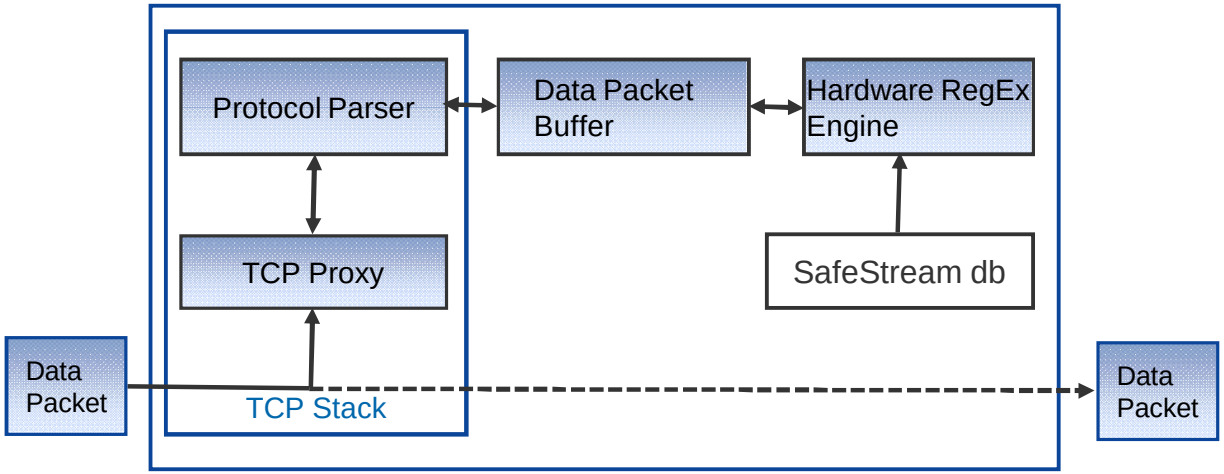
Full AV

- データパケットは、解析され収集されます。
- ファイルを再構築します。(最大20/30Mb)
- ファイルは、処理されるために、AVエンジンに送られます。



Express AV

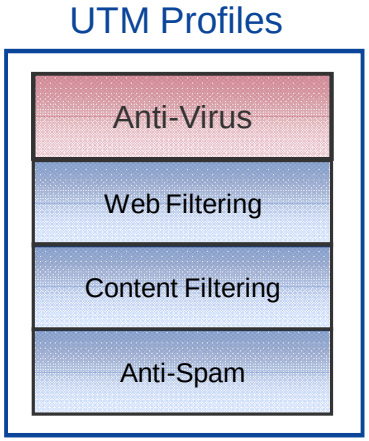
- データパケットは、解析され、バッファされます。
- バッファされたデータは、AVエンジンに送られます。
- ファイル全体を再構築する必要は、ありません。



EXPRESS AV 対応モデル/ライセンス対応

Branch Model	Base Memory(BM) (基本モデル)	High Memory(HM) (UTM対応モデル)	Notes
SRX100	×	× (HMにUpgradeは可能だが、 ExpressAVには非対応)	ExpressAVは使用不可
SRX210	×	○	BM->HMへのUpgradeは不可 (購入時に指定) HMでのみExpressAV使用可能
SRX240	×	○	BM->HMへのUpgradeは不可 (購入時に指定) HMでのみExpressAV使用可能
SRX650	N/A	○ HMのみ販売	全てのSRX650で利用可能

アンチウィルス

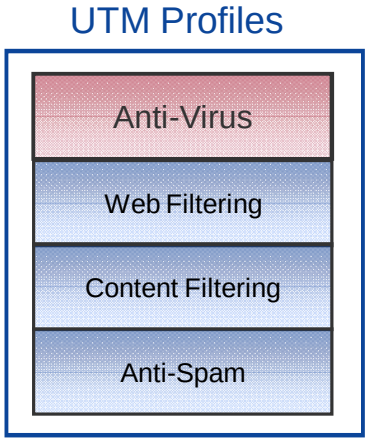


URL ホワイトリストは、サイトから、トラフィックのスキャンをバイパスするために、利用することができます。

MIMEリストは、トラフィックスキャンのバイパスを設定することができます。

- text/html
- text/css
- audio/
- video/
- image/
- application/pdf
- application/x-director

アンチウィルス



AV プロファイルの設定:

- トリクリング オプション
- スキャン オプション
- 通知 オプション
- フォールバック オプション

ウェブ フィルタリング

統合型のサーフコントロールソリューションと、リダイレクト型のウェブセンスのソリューションおよびローカルフィルタリングソリューションを提供しています。

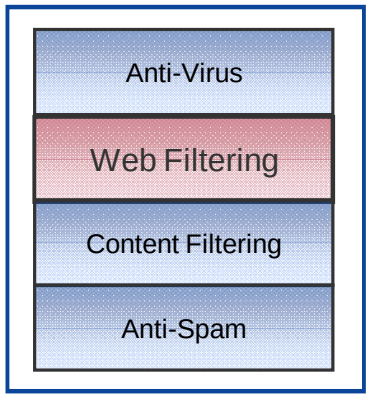
ホワイトリスト/ブラックリストを設定することができます。

統合型ソリューションは、各々のURLのカテゴリを取得するために、サーフコントロールサーバへクエリーを送信します。許可/不許可の決定は、SRXのフィルタープロファイルをベースに作られます。

- カスタムカテゴライズ(ユーザがカスタマイズできます)
- URLカテゴライズ(以下URLからカテゴリされているサイトがわかります)
  - http://mtas.surfcontrol.com/mtas/JuniperTest-a-Site.asp

リダイレクト型ソリューションは、フィルターポリシーを設定しているウェブセンスのサーバに、全てのウェブトラフィックをリダイレクトさせる必要があります。

ローカルフィルタリングソリューションは、ライセンスなしで使用できます。

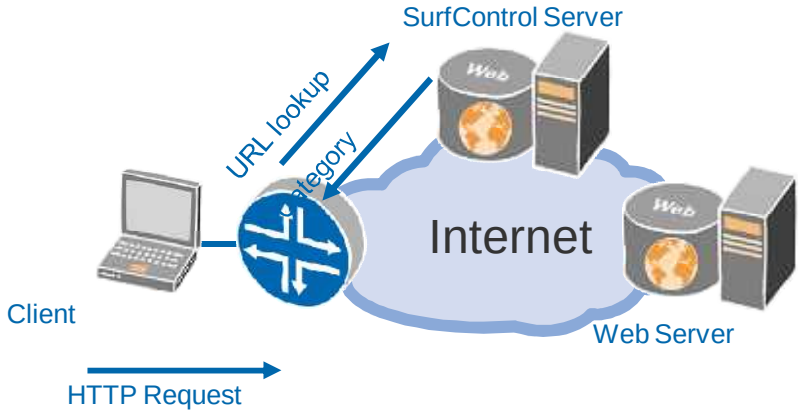


(注) サーフコントロール社はウェブセンス社に買収されていますが、便宜上2つを分けて記載しています。

統合型 & リダイレクト型 WF ソリューション

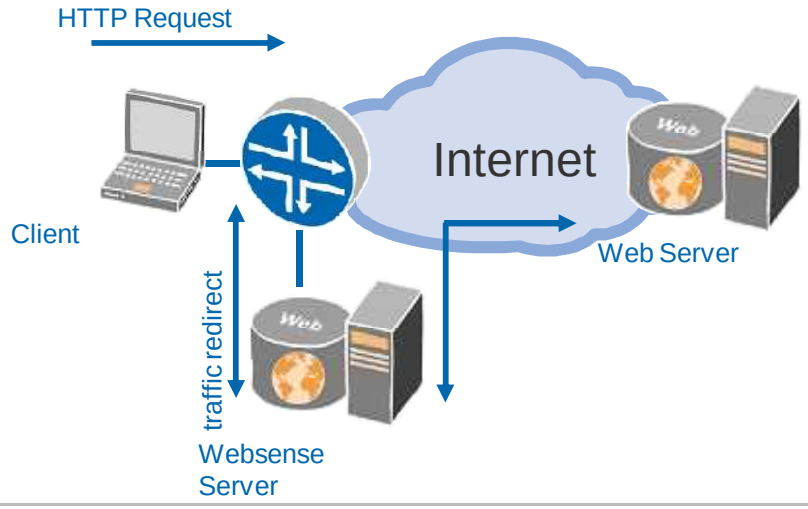
統合ウェブフィルタリング

- サーフコントロール(SC)インターネットスレッドDBがベースです。
- 260万URL以上、40カテゴリ、70言語以上、日々アップデートされています。
- ファイルは、処理のためにAVエンジンに、送られます。
- 許可/不許可は、SCサーバから受け取ったカテゴリを利用し、ローカルのポリシーに基づいて決定されます。



リダイレクト型ウェブフィルタリング

- ウェーブセンスマスターDBがベースです。
- 220万URL以上、95カテゴリー、100以上のプロトコルをサポートしています。 (incl. IM, P2Pなど)
- ポリシーを施工しているサーバに、HTTPトラフィックをリダイレクトさせる必要があります。



統合型 VS. リダイレクト型　WF

使いやすさ

- 統合型は、サーフコントロールのサーバを利用するために、利用しやすいです。一方、リダイレクト型は、ウェブセンスのソフトウェアをインストールしたサーバを構築するため、統合型より、手間がかかります。

遅延

- サーフコントロールへのサーバアクセスが必要になるため、統合型の方が、遅延が大きいです。

統合型 と リダイレクトWFの使い分け

- 簡易にWFを実施したいのであれば、統合型WF
- 遅延を気にするのであれば、リダイレクト型WF

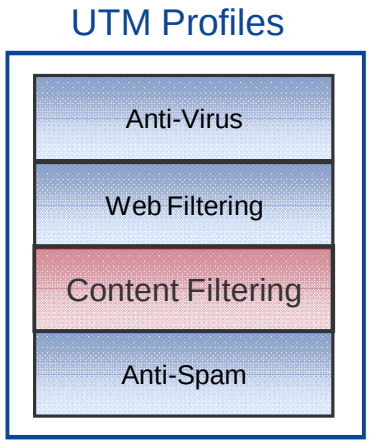
コンテンツ フィルタリング

トラフィックの許可/不許可を、以下をベースに決定します。

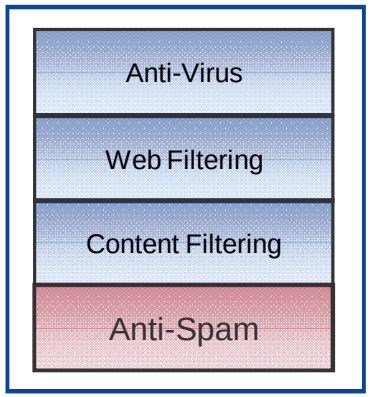
- MIMEタイプ
- ファイル拡張子
- プロトコルコマンド

上記に加えて、HTTPのコンテンツフィルタリングは、以下のプロトコルをブロックできます。

- JAVA
- ActiveX
- Cookies
- ZIPファイル
- EXEファイル



アンチスパム



送信者のIPアドレスの評価をベースにホストサービスを提供します。

スパムブラックリストデータベース – シマンテック SBL/ RBL (スパム/ リアルタイム /ブラックリスト)

SMTPトラフィックのみ設定できます。

IPアドレス、ドメイン名、メールアドレスを元に、グローバル ホワイトリスト/ブラックリストの設定を許可します。

SMTPのネゴシエーションから、送信者のIPアドレス、ドメイン名を取得します。

- 送信者のドメイン名とIPアドレスは、ホワイトリスト/ブラックリストをチェックするために、使われます。
- 送信者のIPアドレスは、SBLに対してチェックされます。

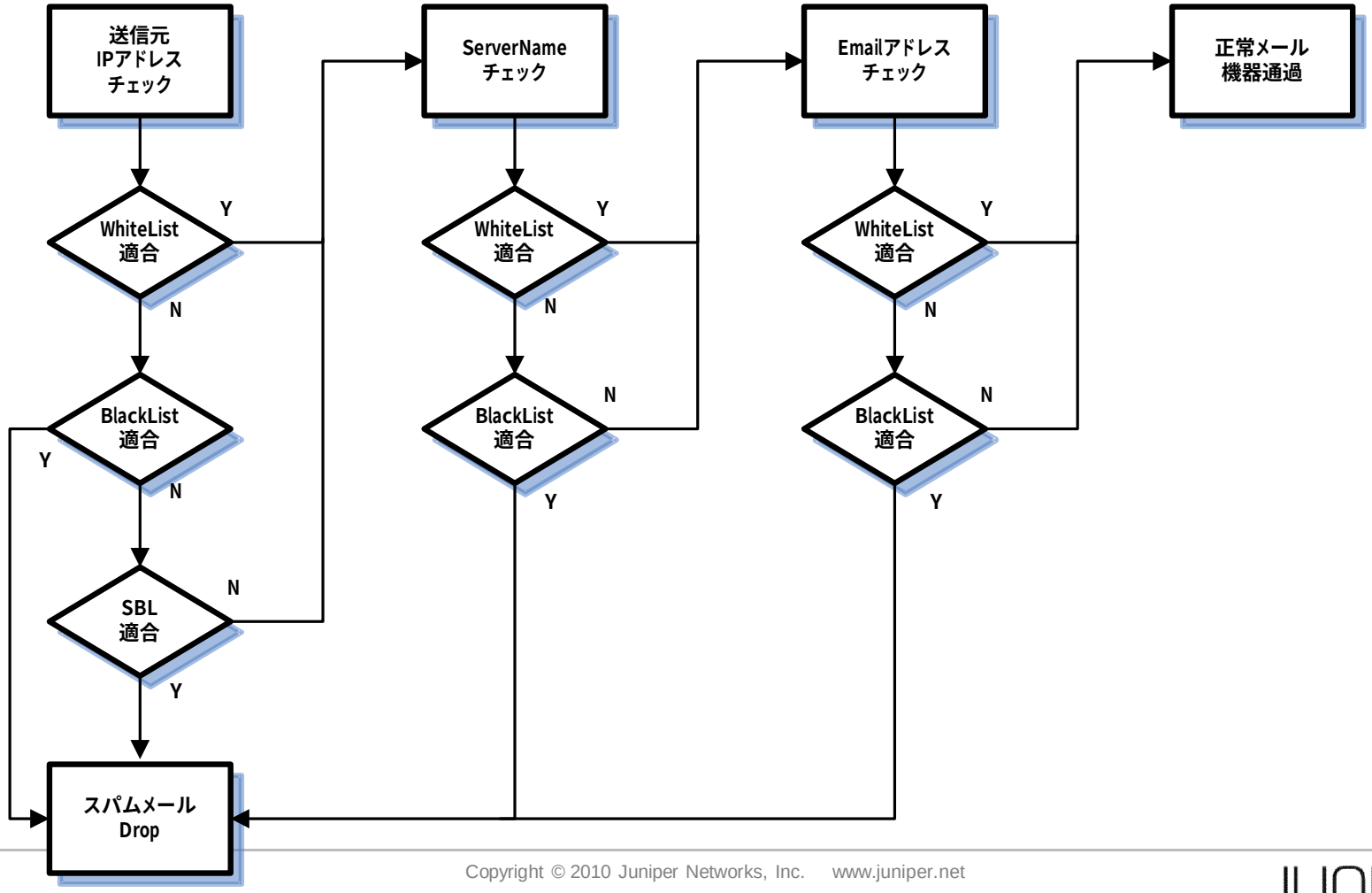
ジュニパーのセキュリティウェブサイトには、デイリートップ100のリストを公開しています。

SBLにリストされているIPアドレスの削除申請は、以下URLで行えます。

- *http://ipremoval.sms.symantec.com/lookup/*

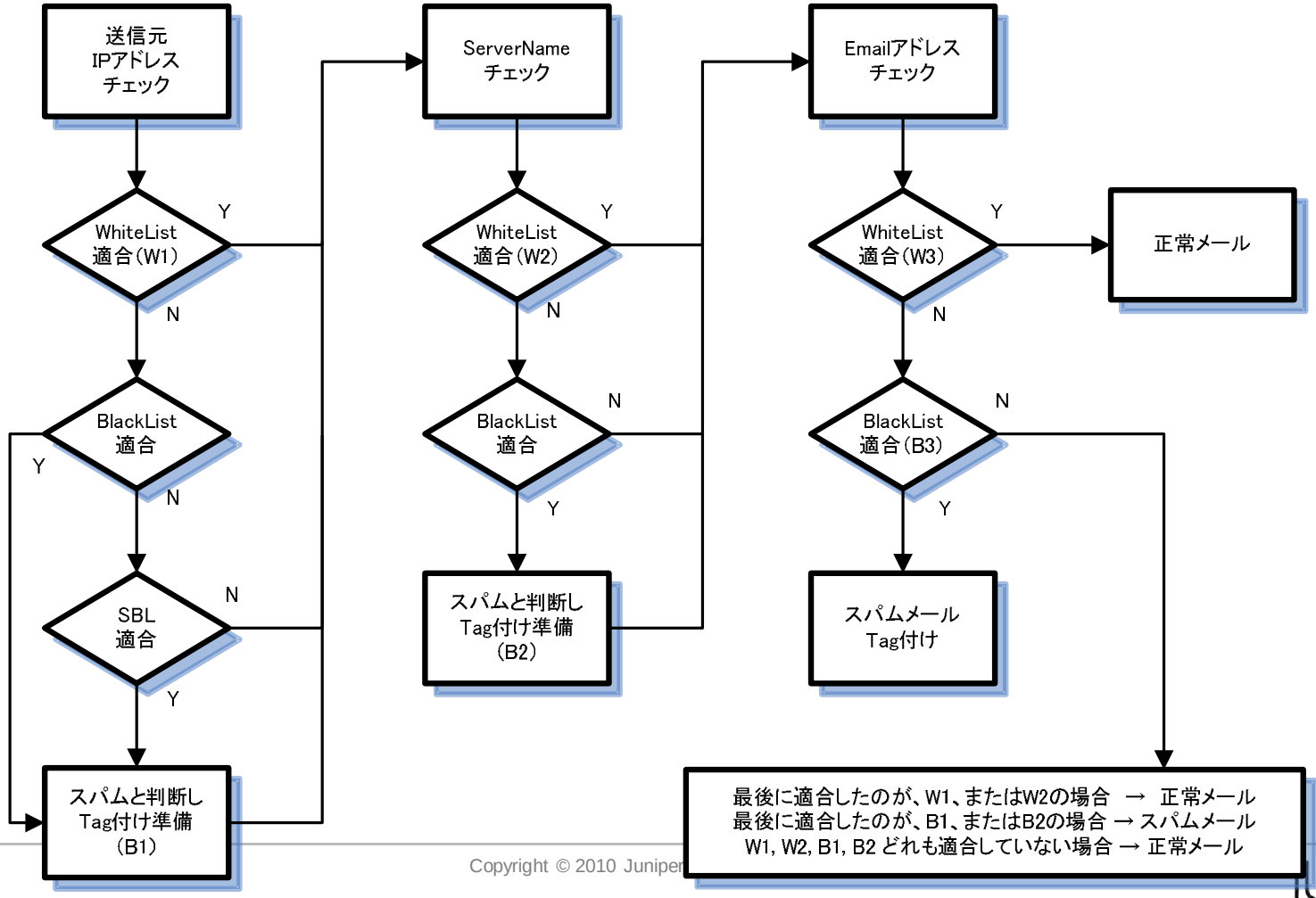
DROPモード時のスパム判定フロー

Black-List、SBLに適合した時点でメールをDropします。



TAGモード時のスパム判定フロー

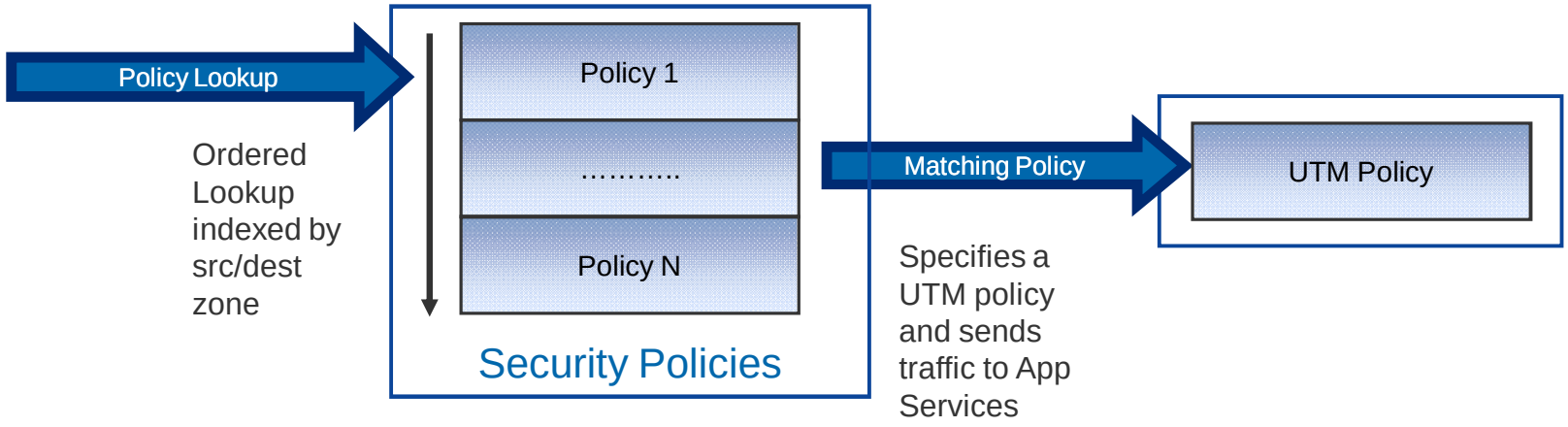
最後に適合した項目で、スパムメールか判定します。



UTMポリシー

セキュリティポリシーは、UTMモジュールで処理するべきトラフィックを判断し、UTMポリシーに送り出します。セキュリティポリシーにおいて、UTM機能が有効になっている必要があります。

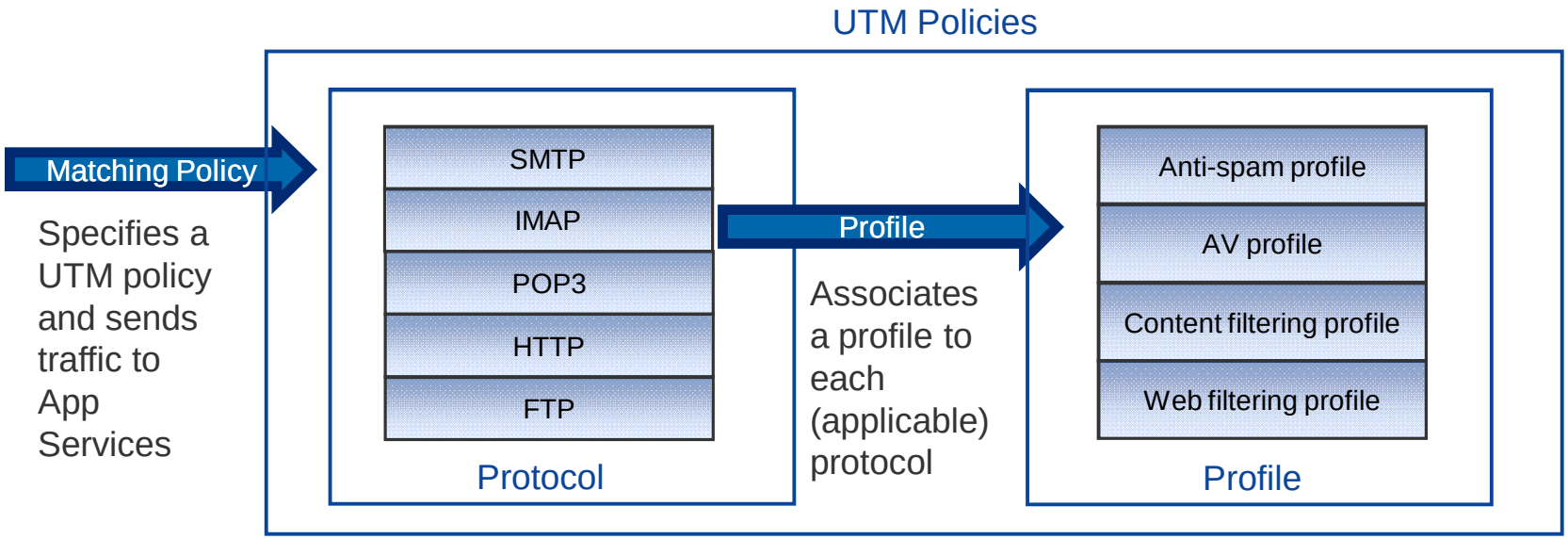
UTMポリシーは、各プロトコル(HTTP、SMTPなど)とUTM機能(AV、ASなど)を関連付けます。



UTMポリシー

UTM ポリシーは、各々のプロトコルにフューチャープロファイルを割り当てます。

フュチャープロファイルは、各々のUTM機能(コンテンツフィルタリング、ウェブフィルタリング)の設定を特定します。



アンチウィルス(EXPRESS AV)設定手順 ①

ライセンスの確認

```
lab@srx-1> show system license
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  av_key_kaspersky_engine               1            1           0    2010-10-16 00:00:00 UTC
  anti_spam_key_sbl                     0            1           0    2010-10-16 00:00:00 UTC
  wf_key_surfcontrol_cpa                0            1           0    2010-10-16 00:00:00 UTC
  idp-sig                               0            1           0    2010-10-16 00:00:00 UTC
  dynamic-vpn                           0           11           0    2010-10-16 00:00:00 UTC
  ax411-wlan-ap                         0            2           0    permanent


  License identifier: JUNOS268959
  License version: 2
  Valid for device: AN4409AA0013
  Features:
    av_key_kaspersky_engine - Kaspersky AV
      date-based, 2010-08-17 00:00:00 UTC - 2010-10-16 00:00:00 UTC
```

各種ライセンスのインストール方法 <参考>

ライセンスのインストール方法

```
lab@srx-1> request system license add terminal
[Type ^D at a new line to end input,
 enter blank line between each license key]
JUNOS268959 aeaqea qmifhd inbqhf aucmbq gezqqb qcdg47
            norsa4 ucq5kc wws2gb 63yfki x5bjz2 iqdgpw
            7jgftl yh2uez xajsga jqu4i3 mrr5l4 oryw3y
            qpa
JUNOS268959: successfully added
add license complete (no errors)


lab@srx-1> request system license add /var/tmp/license


lab@srx-1> request system license update
Request to automatically update license keys from
https://ae1.juniper.net has been sent, use 'show system license' to
check status.
```

ターミナルからインストール

ライセンスキーをターミナルに、ペースト

ライセンスファイルを任意の場所に格納し、インストール

ライセンスサーバーからのインストール(要インターネット接続)

アンチウィルス(EXPRESS AV)設定手順 ②

AVエンジンタイプの確認

```
lab@srx-1> show security utm anti-virus status
 UTM anti-virus status:

    Anti-virus key expire date: 2010-10-16 00:00:00
    Update server: http://update.juniper-updates.net/AV/SRX210/
           Interval: 60 minutes
           Pattern update status: next update in 49 minutes
           Last result: download index file failed
    Anti-virus signature version: not loaded
    Anti-virus signature compiler version: N/A
    Scan engine type: kaspersky-lab-engine
    Scan engine information: last action result: Engine not ready
```

エンジンタイプの確認
現状は、Full AV

アンチウィルス(EXPRESS AV)設定手順 ③

```
lab@srx-1# show security utm
feature-profile {
    anti-virus {
        type juniper-express-engine;
    }
}
```

①feature-profileにて、Express AVを選択

```
lab@srx-1# show security utm
utm-policy xxx-policy {
    anti-virus {
        http-profile junos-eav-defaults;
    }
}
```

②utm-policyにて、スキャンするプロトコル、エンジンタイプを選択

```
lab@srx-1# show security policies
from-zone trust to-zone untrust {
    policy trust-to-untrust {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    utm-policy xxx-policy;
                }
            }
        }
    }
}
```

③security policyにて、AVを実行するポリシーに適用

エンジンタイプを切り替えた場合は、リブートが必要です。

アンチウィルス(EXPRESS AV)設定手順 ④

パターンファイルのアップデート

```
lab@srx-1> request security utm anti-virus juniper-express-engine pattern-update
Anti-virus update request results: av_mgr: pattern updater 2471 is started,
downloading from http://update.juniper-updates.net/EAV/SRX210/.


lab@srx-1> show security utm anti-virus status
 UTM anti-virus status:

    Anti-virus key expire date: 2010-10-16 00:00:00
    Update server: http://update.juniper-updates.net/EAV/SRX210/
           Interval: 1440 minutes
           Pattern update status: next update in 1439 minutes
           Last result: already have latest database
    Anti-virus signature version: 071710_01
    Anti-virus signature compiler version: NLML7> compiler sdk version 2.3
    Scan engine type: juniper-express-engine
    Scan engine information: No error
```

最新のパターンファイルになっていることを確認

エンジンのタイプを確認

エンジンが正常に起動していることを確認

ウェブフィルタリング(統合型)設定手順 ①

ライセンスの確認

```
lab@srx-1> show system license
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  av_key_kaspersky_engine               1            1           0    2010-10-16 00:00:00 UTC
  anti_spam_key_sbl                     0            1           0    2010-10-16 00:00:00 UTC
  wf_key_surfcontrol_cpa                0            1           0    2010-10-16 00:00:00 UTC
  idp-sig                               0            1           0    2010-10-16 00:00:00 UTC
  dynamic-vpn                           0           11           0    2010-10-16 00:00:00 UTC
  ax411-wlan-ap                         0            2           0    permanent


 License identifier: JUNOS268961
  License version: 2
  Valid for device: AN4409AA0013
  Features:
    wf_key_surfcontrol_cpa - Web Filtering
      date-based, 2010-08-17 00:00:00 UTC - 2010-10-16 00:00:00 UTC
```

ウェブフィルタリング(統合型)設定手順　②-1

カテゴリーによるウェブフィルタリングの設定

```
lab@srx-1# show security utm
feature-profile {
    web-filtering {
        type surf-control-integrated;
        surf-control-integrated {
            profile xxx-wf-profile {
                category {
                    Computing_Internet {
                        action block; ;
                    }
                }
            }
        }
    }
}
```

①統合型を選択

②feature-profileにて、カテゴリーに応じてアクションを決定する

```
lab@srx-1# show security utm
utm-policy xxx-policy {
    web-filtering {
        http-profile xxx-wf-profile;
    }
}
```

③utm-policyにて、WFを実行するプロファイルを選択

```
lab@srx-1# show security policies
from-zone trust to-zone untrust {
    policy trust-to-untrust {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    utm-policy xxx-policy;
                }
            }
        }
    }
}
```

④security policyにて、WFを実行するポリシーに適用

ウェブフィルタリング(統合型)設定手順　②-2

ブラック/ホワイトリストによるウェブフィルタリングの設定

```
lab@srx-1# show security utm
custom-objects {
    url-pattern {
        badsite {
            value www.badsite.com;
        }
        goodsite {
            value www.goodsite.com;
        }
    }
    custom-url-category {
        good-category {
            value goodsite;
        }
        bad-category {
            value badsite;
        }
```

①ブラック/ホワイトリストに登録するURLを設定

②URL群にカテゴリー名を設定

```
lab@srx-1# show security utm
feature-profile {
   web-filtering {
        url-whitelist good-category;
        url-blacklist bad-category;
        type surf-control-integrated;
        surf-control-integrated {
            profile xxx-wf-profile {
                category {
```

③ブラック/ホワイトリストに追加するカテゴリーを設定

```
lab@srx-1# show security utm
utm-policy xxx-policy {
    web-filtering {
        http-profile xxx-wf-profile;
    }
}
```

④utm-policyにて、WFを実行するプロファイルを選択

```
lab@srx-1# show security policies
from-zone trust to-zone untrust {
    policy trust-to-untrust {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    utm-policy xxx-policy;
                }
            }
        }
    }
}
```

⑤security policyにて、WFを実行するポリシーに適用

ウェブフィルタリング(統合型)設定手順 ③

ステータスの確認

```
lab@srx-1# show security utm web-filtering status
 UTM web-filtering status:
    Server status: SC-CPA server up

[edit]
lab@srx-1# show security utm web-filtering statistics
 UTM web-filtering statistics:
    Total requests:                 0
    white list hit:                 0
    Black list hit:                 0
    Queries to server:              0
    Server reply permit:            0
    Server reply block:             0
    Custom category permit:         0
    Custom category block:          0
    Cache hit permit:               0
    Cache hit block:                0
    Web-filtering sessions in total: 4000
    Web-filtering sessions in use:   0
    Fall back:                      log-and-permit          block
          Default                                0              0
          Timeout                                0              0
     Connectivity                                0              0
Too-many-requests                                0              0
```

ウェブフィルタリングサーバーとの疎通、ステータス確認

コンテンツフィルタリング設定手順　①-1

拡張子のフィルタリング設定

```
lab@srx-1# show security utm
custom-objects {
    filename-extension {
        executables {
            value [ exe dot sys ];
        }
    }

lab@srx-1# show security utm
feature-profile {
    content-filtering {
          profile block-exe {
            block-extension executables;
        }

lab@srx-1# show security utm
utm-policy xxx-policy {
    content-filtering {
        ftp {
            download-profile block-exe;
    }
```

①フィルタリングする拡張子を設定

②feature-profileにて、フィルタリングに応じてアクションを決定する

③utm-policyにて、コンテンツフィルタリングを実行するプロトコルを選択

```
lab@srx-1# show security policies
from-zone trust to-zone untrust {
    policy trust-to-untrust {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    utm-policy xxx-policy;
                }
            }
        }
    }
}
```

④security policyにて、コンテンツフィルタリングを実行するポリシーに適用

コンテンツフィルタリング設定手順 ①-2

FTPコマンドのフィルタリング設定

```
lab@srx-1# show security utm
custom-objects {
    protocol-command {
        ftp-put {
            value STOR;
        }
```

①フィルタリングするコマンドを設定

```
lab@srx-1# show security utm
feature-profile {
    content-filtering {
        profile block-ftp-put {
            block-command ftp-put;
        }
```

②feature-profileにて、フィルタリングに応じてアクションを決定する

```
lab@srx-1# show security utm
utm-policy xxx-policy {
    content-filtering {
        ftp {
            upload-profile block-ftp-put;
    }
```

③utm-policyにて、コンテンツフィルタリングを実行するプロトコルを選択

```
lab@srx-1# show security policies
from-zone trust to-zone untrust {
    policy trust-to-untrust {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    utm-policy xxx-policy;
                }
            }
        }
    }
}
```

④security policyにて、コンテンツフィルタリングを実行するポリシーに適用

コンテンツフィルタリング設定手順 ①-3

ActiveXのフィルタリング設定

```
lab@srx-1# show security utm
feature-profile {
    content-filtering {
       profile block-activex {
           block-content-type {
               activex;
       }
```

① feature-profileにて、フィルタリングするコンポーネントを設定

```
lab@srx-1# show security utm
utm-policy xxx-policy {
    content-filtering {
        http-profile block-activex;
    }
```

②utm-policyにて、コンテンツフィルタリングを実行するプロトコルを選択

```
lab@srx-1# show security policies
from-zone trust to-zone untrust {
    policy trust-to-untrust {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    utm-policy xxx-policy;
                }
            }
        }
    }
}
```

③security policyにて、コンテンツフィルタリングを実行するポリシーに適用

コンテンツフィルタリング設定手順 ②

ステータスの確認

```
lab@srx-1> show security utm content-filtering statistics

 Content-filtering-statistic:          Blocked
     Base on command list:                    1
     Base on mime list:                       0
     Base on extension list:                  0
     ActiveX plugin:                          0
     Java applet:                             0
     EXE files:                               0
     ZIP files:                               0
     HTTP cookie:                             3
```

アンチスパム設定手順 ①

ライセンスの確認

```
lab@srx-1> show system license
License usage:
                                Licenses     Licenses    Licenses    Expiry
  Feature name                       used    installed      needed
  av_key_kaspersky_engine               1            1           0    2010-10-16 00:00:00 UTC
  anti_spam_key_sbl                     0            1           0    2010-10-16 00:00:00 UTC
  wf_key_surfcontrol_cpa                0            1           0    2010-10-16 00:00:00 UTC
  idp-sig                               0            1           0    2010-10-16 00:00:00 UTC
  dynamic-vpn                           0           11           0    2010-10-16 00:00:00 UTC
  ax411-wlan-ap                         0            2           0    permanent


  License identifier: JUNOS268960
  License version: 2
  Valid for device: AN4409AA0013
  Features:
    anti_spam_key_sbl - Anti-Spam
      date-based, 2010-08-17 00:00:00 UTC - 2010-10-16 00:00:00 UTC
```

アンチスパム設定手順 ②

SBLサーバーとブラックリストの併用

```
lab@srx-1# show security utm
custom-objects {
    url-pattern {
        spam-black {
            value "hogehoge@spam.com";
        }
    }

lab@srx-1# show security utm
feature-profile {
   anti-spam {
        address-blacklist spam-black;
        sbl {
            profile sbl-profile {
                sbl-default-server;
                spam-action block;
            }
        }
    }


lab@srx-1# show security utm
utm-policy xxx-policy {
    anti-spam {
        smtp-profile sbl-profile;
    }
```

①ブラックリストに登録するメールアドレスを設定

②ブラックリストに追加するカテゴリーを設定

③SBLサーバーを選択

④スパムメールに対してのアクションを決定

⑤utm-policyにて、アンチスパムを実行するプロトコルを選択

```
lab@srx-1# show security policies
from-zone trust to-zone untrust {
    policy trust-to-untrust {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    utm-policy xxx-policy;
                }
            }
        }
    }
```

⑥security policyにて、アンチスパムを実行するポリシーに適用

アンチスパム設定手順 ②

ステータスの確認

```
lab@srx-1> show security utm anti-spam status
SBL Whitelist Server:
SBL Blacklist Server:
    msgsecurity.juniper.net

DNS Server:
    Primary  :   208.67.222.222, Src Interface: ge-0/0/0
    Secondary:   208.67.220.220, Src Interface: ge-0/0/1
    Ternary  :         0.0.0.0, Src Interface: fe-0/0/2
```

テストコマンド

```
lab@srx-1> test security utm anti-spam test-string IPAdd/Domain/E-mail
```

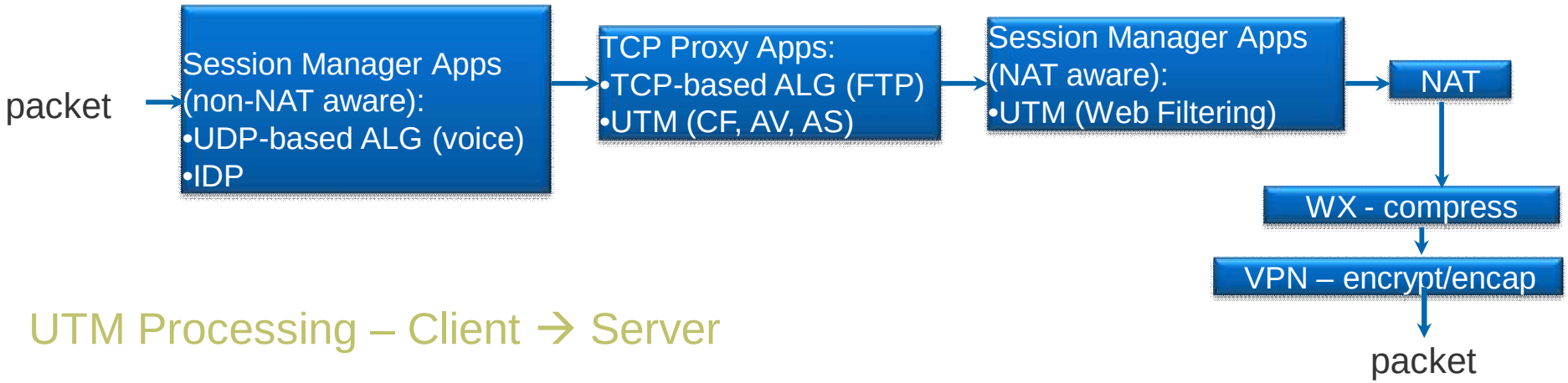
UTMポリシー

フューチャープロファイルの設定とUTMポリシーは連動しています。
UTMポリシーは、複数のセキュリティポリシーに定義できます。
一つのセキュリティーポリシーに複数のプロトコルを定義できます。

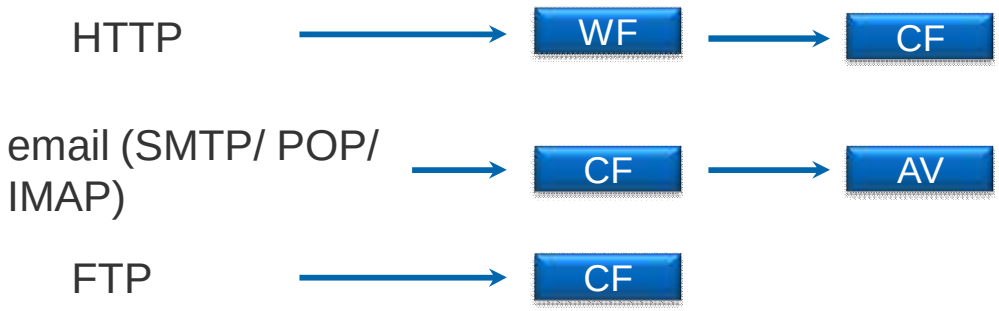
```
lab@srx-1# show security utm utm-policy xxx-policy
anti-virus {
    http-profile junos-eav-defaults;
}
content-filtering {
    http-profile block-activex;
    ftp {
        upload-profile block-ftp-put;
        download-profile block-exe;
    }
}
web-filtering {
    http-profile xxx-wf-profile;
}
anti-spam {
    smtp-profile sbl-profile;
}
```

UTM SERVICE – パケット処理 <クライアントからサーバー>

Client → Server

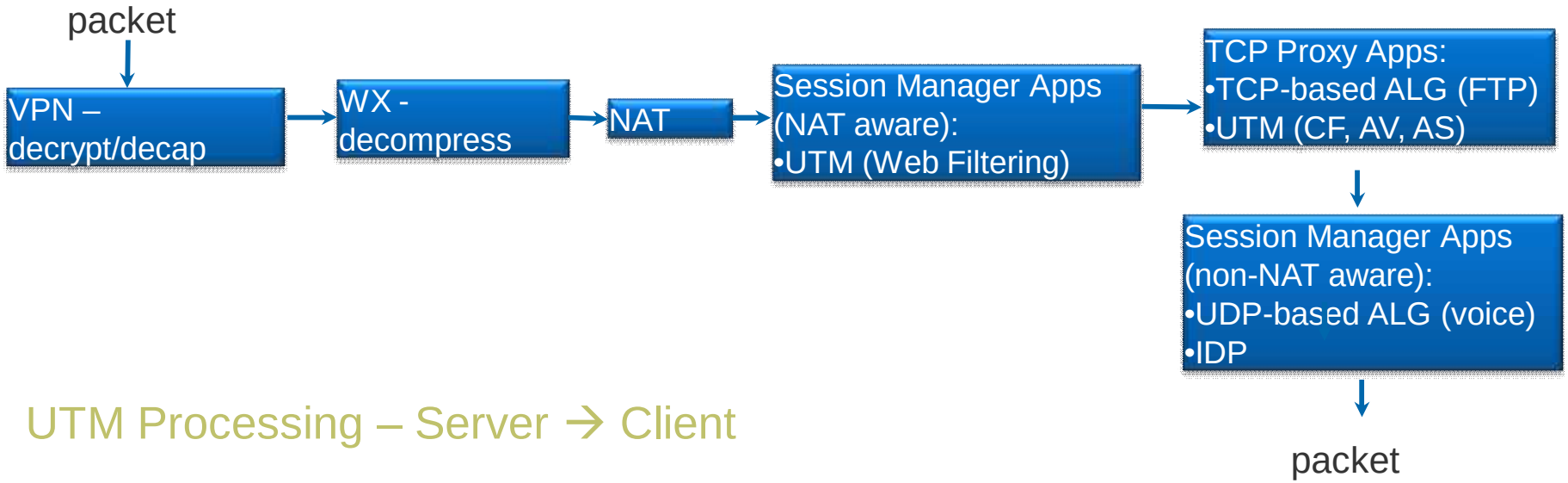


UTM Processing – Client → Server

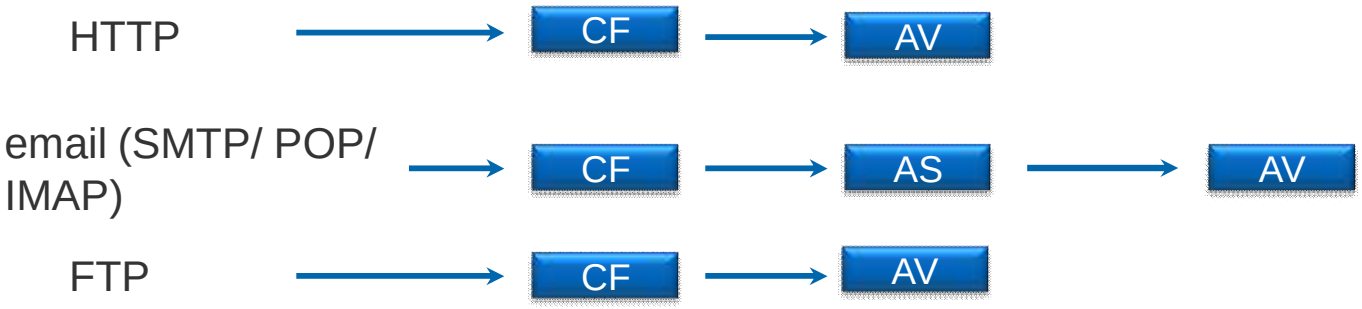


UTM SERVICE – パケット処理 <サーバーからクライアント>

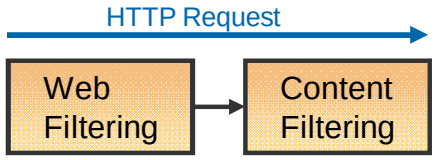
Server → Client



UTM Processing – Server → Client

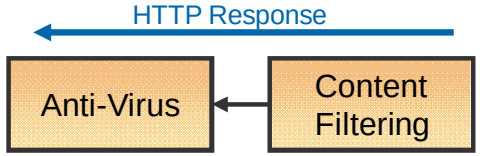


UTM トラフィック処理: HTTP



HTTP Request

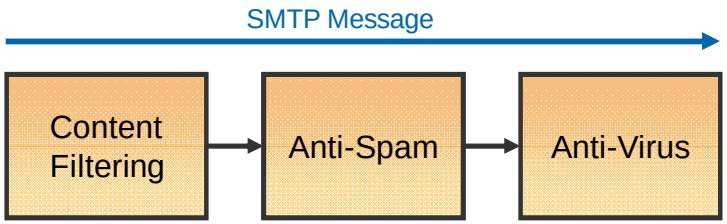
- Web Filtering -> Content Filtering:：はじめに、Webフィルタリングで、HTTPリクエストに含まれているURLをチェックします。URLが許可されたら、次に、コンテンツフィルタリングで、HTTPコマンドをチェックします。



HTTP Response

- Content filtering -> Anti-Virus：HTTPレスポンスを、Webフィルターは、HTTPレスポンスのチェックはしません。HTTPレスポンスを受け取った時、はじめに、コンテンツフィルターモジュールは、HTTPレスポンスメッセージの内容をチェックします。許可されれば、アンチウィルスモジュールは、トラフィックをスキャンします。

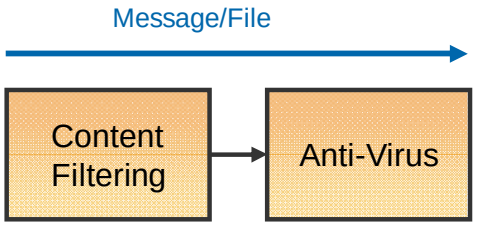
UTM トラフィック処理: SMTP



SMTP Message

- Content Filtering: FWでSMTPトラフィックを受け取った時、コンテンツフィルタリングは、SMTPコマンドをチェックします。
- Anti-Spam: コマンドが許可された時、アンチスパムモジュールに転送されます。Eメールヘッダーを受信した時、アンチスパムモジュールは、スパムデータベースに問い合わせをします。
- Anti-Virus: Eメールがスパムでない、または、ユーザーがスパムに対して、Eメールにタグを選択した時、アンチウィルスモジュールにより、Eメールボディは、スキャンされます。
  - アンチウィルスモジュールで、Express AVを選択している時、スパムモジュールがEメールヘッダーをチェックしている時でも、アンチウィルスモジュールは、スキャンを開始します。

UTM トラフィック処理: FTP、 POP、 IMAP



その他のプロトコル

- **他のプロトコル(FTP、POP、IMAPなど)に関して、はじめに、コンテンツフィルタリングが、プロトコルコマンドをチェックします。プロトコルコマンドで許可されたら、次は、そのプロトコルで運ばれてきたコンテンツを、アンチウィルスモジュールにて、スキャンを開始します。**

everywhere